

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK**

ROBERT D’AGOSTINI, individually and  
on behalf of all others similarly situated,

Plaintiff,

v.

EMPRESS AMBULANCE SERVICE, LLC  
d/b/a EMPRESS EMS, a Delaware limited  
liability company; DOES 1 to 100,  
inclusive,

Defendant.

Civil Action No.: 22-cv-10122

**CLASS ACTION COMPLAINT**

1. Negligence
2. Breach of Implied Contract
3. Violation of New York Gen. Bus. Law  
§349

**DEMAND FOR JURY TRIAL**

**CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff ROBERT D’AGOSTINI (“Plaintiff”), individually and on behalf of all others similarly situated, brings this action against Defendant EMPRESS AMBULANCE SERVICE, LLC d/b/a EMPRESS EMS (“Defendant” or “Empress”) based upon personal knowledge as to himself and his own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of his attorneys.

**NATURE OF THE ACTION**

1. In or around May 26, 2022, Empress experienced a data breach whereby unauthorized, third-party hackers gained access to Defendant’s internal systems through a ransomware attack. Empress did not detect this unauthorized access until July 14, 2022—almost two months later—at which point those third-party hackers had already exfiltrated the personal identifying information (“PII”) and protected health information (“PHI”) of approximately 318,558 individuals from Empress’ systems. This PII included, *inter alia*, those individual’s

names, dates of birth, demographic information, diagnosis and treatment information, medical record numbers, dates of service, insurance information, prescription information, and social security numbers.

2. Empress is an emergency medical services and aftercare transportation provider in the New York metro area. As part of its business operations, Empress collects and stores the PII and PHI of patients who use its services.

3. Under statute and regulation, Empress had a duty to implement reasonable, adequate industry-standard data security policies safeguards to protect patient PII and PHI. Empress acknowledges that it is bound by these duties in its “Privacy Practices Statement” posted on its website.<sup>1</sup> Despite this, Empress failed to implement such reasonable and adequate data safeguards and allowed third-party hackers to exfiltrate its patients’ PII and PHI.

4. Plaintiff, individually and on behalf of those similarly situated persons (hereafter “Class Members”), bring this Class Action to secure redress against Empress for its reckless and negligent violation of their privacy rights. Plaintiff and Class Members are patients and former patients of Empress who had their PII and PHI collected, stored and ultimately breached by Empress.

5. Plaintiff and Class Members have suffered injuries and damages. As a result of Empress’s wrongful actions and inactions, Plaintiff and Class Members’ names, dates of birth, demographic information, diagnosis and treatment information, medical record numbers, dates of service, insurance information, prescription and treatment information, medical record numbers, dates of service, insurance information, prescription information, and social security numbers have all been compromised. Plaintiff and Class Members have had their privacy rights violated and are now exposed to a heightened risk of identity theft and credit fraud for the remainder of their lifetimes. Plaintiff and Class Members must now spend time and money on prophylactic measures, such as increased monitoring of their personal and financial accounts and the purchase of credit

---

<sup>1</sup> “Notice of Privacy Practices” <https://empressems.com/wp-content/uploads/2022/07/empressprivacy.pdf> (lasted accessed November 8, 2022).

monitoring services, to protect themselves from future loss. Plaintiff and Class Members have also lost the value of their PII and PHI.

6. Further, Empress unreasonably delayed in notifying Plaintiff and Class Members of the data breach until approximately September 9, 2022—despite having discovered the breach nearly two months earlier—when it disseminated letters informing Plaintiff and other Class Members that their PII and PHI had been compromised by the data breach (the “Data Breach Notice”).

7. Even more egregiously, Empress’s Data Breach Notice sent to Plaintiff omits and misrepresents key information about the data breach. The Data Breach Notice did not disclose that the Hive Gang (“Hive”), a notorious ransomware group, had announced that they were behind the breach. Immediately following the data breach, Hive contacted Defendant by email, in which they claimed that they had downloaded Empress’ “most important information with a total size over 280 GB,” and claimed to have obtained over 100,000 social security numbers from Empress’ systems.<sup>2</sup> This is in stark contrast to Empress’ Data Breach Notice and public disclosures, in which they claimed that only “a small subset of files” had been copied.<sup>3</sup>

8. Empress’ Data Breach Notice also failed to inform Plaintiff that the Empress data breach had been briefly listed on Hive’s leak website, and that files exfiltrated in the data breach have been discovered available for download on the dark web.<sup>4</sup>

9. As a result of Empress’s wrongful actions and inactions, patient information was stolen. Plaintiff and Class Members have had their PII and PHI compromised by nefarious third-party hackers, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Plaintiff and Class Members bring this action to secure redress against Empress.

---

<sup>2</sup>“NY: Empress EMS hit by Hive ransomware” <https://www.databreaches.net/ny-empress-ems-hit-by-hive-ransomware/> (last accessed November 8, 2022).

<sup>3</sup> “Notice of Security Incident” <https://empressems.com/notice-of-security-incident/> (last accessed November 8, 2022).

<sup>4</sup> “Hive Ransomware Victim: Empress EMS” <https://www.redpacketsecurity.com/hive-ransomware-victim-empress-ems/> (last accessed November 8, 2022).

### **THE PARTIES**

10. Plaintiff Robert D'Agostini is a New York citizen residing in Yonkers, New York. Plaintiff is a former patient of Empress who provided his PII and PHI to Empress in connection to receiving healthcare services from Empress. On or around September 9, 2022, Plaintiff received a data breach notice from Empress informing him that documents containing his name, social security number, date of service and name of his insurer had been obtained by unauthorized third-party hackers.

11. Defendant Empress Ambulance Service, LLC d/b/a Empress EMS is a Delaware limited liability company with its principal place of business at 722 Nepperhan Ave, Yonkers, New York, 10703. Empress is registered as its own agent for service of process.

12. Plaintiff is unaware of the true names, identities, and capacities of the defendants sued herein as DOES 1 to 100. Plaintiff will seek leave to amend this Complaint to allege the true names and capacities of DOES 1 to 100 if and when ascertained. Plaintiff is informed and believes, and based thereon alleges, that each of the defendants sued herein as a DOE is legally responsible in some manner for the events and happenings alleged herein and that each of the defendants sued herein as a DOE proximately caused injuries and damages to Plaintiff and Class members as set forth below.

### **JURISDICTION AND VENUE**

13. This Court has subject matter jurisdiction over the claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), since Plaintiff is a citizen of a State different from the Defendant and, upon the original filing of this complaint, there are more than 100 putative class members in this action and the amount in controversy exceeds \$5 million.

14. The Court also has personal jurisdiction over the Parties because Defendant routinely conducts business in New York and has sufficient minimum contacts in New York to have intentionally availed themselves to this jurisdiction by operating and providing services in New York.

15. Venue is proper in the Southern District because, among other things: (a) Plaintiff

Robert D’Agostini is a resident of this District and a citizen of this state; (b) Defendant directed its activities at residents in this District; and (c) many of the acts and omissions that give rise to this Action took place in this judicial District.

16. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because, among other things: (a) Plaintiff resides in the Southern District, (b) Defendant conducts substantial business in the Southern District, (c) Defendants directed their services at residents in the Southern District; and (d) many of the acts and omissions that give rise to this Action took place in the Southern District.

## FACTUAL ALLEGATIONS

### A. The Data Breach

17. Empress is a HIPAA covered entity that provides emergency medical services and aftercare transportation to its patients. According to Empress’s website, it is “one of the largest, most experienced emergency and non-emergency response providers in Westchester, Rockland, Ulster, Dutchess, Putnam, Orange County, and the Bronx.”<sup>5</sup> Empress further purports to have retained over 700 “professionally trained and highly skilled” personnel, as well as a 24-hour communications center “[h]ousing one of the most advanced computer aided systems in the region.” In providing its services, Empress collects and stores patient PII and PHI from its patients. As a result, Empress’s systems store the PII and PHI of hundreds of thousands of New York residents who have used its services.

18. On or around May 26, 2022, Empress’s systems suffered a ransomware attack, wherein unauthorized third-party hackers encrypted Empress’ internal systems and exfiltrated Plaintiff’s and Class Members’ sensitive PII and PHI—including, but not limited to, their names, dates of birth, demographic information, diagnosis and treatment information, medical record numbers, dates of service, insurance information, prescription and treatment information, medical record numbers, dates of service, insurance information, prescription information, and social

---

<sup>5</sup> <https://empressems.com/> (last accessed November 8, 2022).

security numbers. Empress did not detect this data breach until July 14, 2022—nearly two months later. During that time, unauthorized third-party hackers had full and unfettered access to Empress’s internal data systems, including its records of patient PII and PHI. In its data breach report filed the United States Secretary of Health and Human Services, Empress reported that the data breach had affected 318,558 individuals.

19. Ransomware is a form of malware designed to gain unauthorized access to and encrypt files on a device or server, rendering any files and the systems that rely on them unusable. Malicious actors use ransomware to unlawfully obtain private, sensitive and/or confidential information, and then demand a ransom in exchange for decrypting the affected files. Ransomware attacks are often targeted towards businesses such as Empress, that are known to collect and store confidential and sensitive PII/PHI of hundreds of thousands of individuals. Ransomware attacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards and/or proper employee cybersecurity training, as the vast majority of ransomware incidents are caused by poor user practices, lack of cybersecurity training, and weak passwords or access management.<sup>6</sup> For instance, ransomware is most commonly spread through “phishing” emails that contain malicious attachments or where an employee visits an infected website on a device connected to a company server. As such, businesses with adequate and reasonable data security practices train their employees not to open email attachments from unrecognized emails or visit unauthorized websites on company device.

20. On July 14, 2022, Empress was contacted through email by the ransomware group the Hive Gang, who informed Empress that it had successfully launched a ransomware attack on Empress’ network and data systems. Hive is a highly sophisticated and prolific ransomware hacking group known to harvest and sell stolen data from businesses that leave vulnerabilities in their cybersecurity. Hive’s July 14, 2022 message read, in-part:

---

<sup>6</sup> “Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020.” Statista, <https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/> (last accessed November 9, 2022).

!!! DO NOT TRY TO DECRYPT OR CHANGE ENCRYPTED FILES ON YOUR COMPUTERS, IT WILL COMPLETELY DESTROY THEM !!!

Ladies and gentlemen! Attention, please!  
This is HIVE ransomware team.

We infiltrated your network and stayed there for 12 days (it was enough to study all your documentation and gain access to your files and services), encrypted your servers.

Downloaded most important information with a total size over 280 GB

Few details about information we have downloaded:

- contracts, nda and other agreements documents
- company private info (budgets, plans, investments, company bank statements, etc.)
- employees info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.)
- customers info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.)
- SQL databases with reports, business data, customers data, etc.
- approximate number of personal records including addresses and ssn's data is above 10000 units<sup>7</sup>

21. Hive would contact Empress again on July 15, 2022, providing them with a sample of the files that they had exfiltrated from its servers. Those files contained the PII and PHI of some of Empress' patients, demonstrating that Hive had indeed gained access to Defendant's customer files. Hive went on to claim that it had obtained more than 100,000 social security numbers from Empress' servers.

22. Shortly following the data breach, Empress was listed briefly on Hive's "HiveLeaks" website, a dark web website wherein Hive publishes a list of its victims that have not settled the ransom to decrypt their hacked systems. Further, files exfiltrated from Empress' internal systems have been discovered available for download on the dark web.

### **B. Empress's Unreasonably Delayed and Inadequate Notification**

23. Empress owed Plaintiff and Class Members a duty under state law to provide timely notification of the data breach. The New York Information and Security Breach and Notification

---

<sup>7</sup> "NY: Empress EMS hit by Hive ransomware" <https://www.databreaches.net/ny-empress-ems-hit-by-hive-ransomware/> (last accessed November 8, 2022).

Act, General Business Law §899-AA (2) provides any business which conducts business in New York and which collects computerized private information must disclose any data breach to “any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization,” and that such disclosure must have been “in the most expedient time possible and without reasonable delay.” Empress did not disclose the data breach to Plaintiff and Class Members in the most expedient time possible, and instead unreasonably delayed almost two months before sending out their Data Breach Notice.

24. Further, the Data Breach Notice sent to Plaintiff also withheld and misrepresented multiple key details regarding the data breach. The Data Breach Notice did not disclose that the identity of the third-party hackers that had acquired Plaintiff’s information had been identified as a highly sophisticated criminal hacking group, and did not inform Plaintiff that customer information stolen in the data breach had already been disseminated on the dark web. Even more egregiously, the Data Breach Notice intentionally downplayed the severity of the breach, claiming that only a “small subset of files” had been compromised. In fact, Hive had obtained over 280 gigabytes of data from Empress’ systems, including the social security numbers of over 100,000 individuals.

25. As a result of Empress’s delayed and inadequate notification, Plaintiff and Class Members were left unaware that their PII had been compromised for almost two months, and many Class Members likely remain unaware of the true nature and extent of the data breach.

### **C. Empress’s Representations That it Would Provide Reasonable, Adequate, and Compliant Data Security**

26. Empress’s “Notice of Privacy Practices” promises that:

Empress Ambulance Service, Inc. is committed to protecting your personal health information. We are required by law to maintain the privacy of health information that could reasonably be used to identify you, known as “protected health information” or “PHI.” We are also required by law to provide you with the attached detailed Notice of Privacy Practices (“Notice”) explaining our legal duties and privacy practices with respect to your PHI.

We respect your privacy and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times.<sup>8</sup>

27. Empress clearly recognized its duty to provide reasonable data security for Plaintiff's and Class Members' PII/PHI that it collects and stores as part of its business practices. Defendant made promises to do protect Plaintiff's and Class Member's PII/PHI in accordance with statute and regulation. Despite this, on information and belief, Empress did not implement the requisite data security safeguards and protocols to protect Plaintiff's and Class Members PII/PHI.

#### **D. Empress's Obligation to Protect Patient PII/PHI Under Federal Law**

28. As a HIPAA covered entity, Empress holds a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Member's PII/PHI.

29. Under the HIPAA Privacy Rule, Empress is required to, *inter alia*:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives maintains or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance with the above data security procedures by their workforce.

45 CFR §164. 306(a)

30. The HIPAA Privacy Rule also requires Empress to “review and modify the security measures implemented...as needed to continue provision of reasonable and appropriate protection of electronic protected health information” under 45 C.F.R. §164.306(e) and to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have

---

<sup>8</sup> “Notice of Privacy Practices” <https://empressems.com/wp-content/uploads/2022/07/empressprivacy.pdf> (lasted accessed November 8, 2022).

been granted access rights” under 45 C.F.R. §164.312(a)(1).

31. Further, the Federal Trade Commission Act, 45 U.S.C. §45 prohibits businesses such as Empress from engaging in “unfair or deceptive acts or practices affecting commerce.” The Federal Trade Commission (“FTC”) has found that a company’s failure to maintain reasonable and appropriate data security for the consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir. 2015).

32. Empress has failed to comply with each of these federal statutes by failing to implement and maintain reasonable security procedures to protect Plaintiff and Class Members’ PII/PHI.

#### **E. Empress’ Failure to Comply with Industry Data Security Standards and Regulations**

33. Experts in the field of data security are in consensus that healthcare providers such as Empress are specifically targeted by hackers due to the value of the PII/PHI that they collect and maintain as a part of their ordinary course of business. As such, experts have identified several best practices that healthcare providers such as Empress should implement and follow in order to best protect themselves from unauthorized access.

34. Such best practices are outlined in the National Institute of Standards and Technology’s (“NIST”) “Security and Privacy Controls for Information Systems and Organizations” publication. These best practices include, *inter alia*, maintaining a plan of action for preventing and addressing data breaches, training and educating employees on data security, implementing strong password requirements, implementing multi-layer security such as two-factor authentication, installation and maintenance of firewalls, anti-virus and anti-malware software, implementing data encryption, monitoring and protection of web browsers and email management systems, and limiting the number of employees with access privileges to patient PII/PHI. *See, e.g.,* NIST SP 800-53, Rev. 5 AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AT-1, AT-3, CA-1, CA-2, CA-3, CA-7, IA-1, IA-2, IA-3, PL-1, PL-2, PM-1, PT-1, PT-2, PT-3.

35. The FTC has also promulgated numerous guides for business which highlight the

importance of implementing reasonable data security practices. In 2016, the FTC updated its publication, “Protecting Personal Information: A Guide for Business,” which establishes guidelines for fundamental data security principles and practices for business.<sup>9</sup> Among other things, the guidelines dictate businesses should protect any personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses implement an intrusion detection system to expose breaches as soon as they occur; monitor all incoming traffic for activity indicating someone is attempting to infiltrate or hack the system; monitor instances when large amounts of data are transmitted to or from the system; and have a response plan ready in the event of a breach.<sup>10</sup> Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.<sup>11</sup>

#### **F. Applicable Standards of Care**

36. In addition to their obligations under federal law and regulation, Empress owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Empress owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer system and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiff and Class

---

<sup>9</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>. (last accessed November 8, 2022).

<sup>10</sup> *Id.*

<sup>11</sup> Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015) <https://www.ftc.gov/business-guidance/resources/start-security-guide-business>. (last accessed November 8, 2022).

Members.

37. Empress owed a duty to Plaintiff and the Class Members to design, maintain, and test their computer system to ensure that the PII/PHI in Defendants' possession was adequately secured and protected.

38. Empress owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in their possession, including adequately training their employees and others who accessed the PII/PHI in their possession, including adequately training their employees and others who accessed PII/PHI in their computer systems on how to adequately protect PII/PHI.

39. Empress owed a duty of care to Plaintiff and Class Members to implement processes that would detect a breach of their data security systems in a timely manner.

40. Empress owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

41. Empress owed a duty to Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft because such an inadequacy would be a material fact in the decision to provide or entrust their PII/PHI to Empress.

42. Empress owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when the data breach occurred.

43. Empress owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Empress received PII/PHI from Plaintiff and Class Members with the understanding that Plaintiff and Class Members expected their PHI/PII to be protected from disclosure. Defendants knew that a breach of its data systems would cause Plaintiff and Class Members to incur damages.

**G. Stolen Information Is Valuable to Hackers and Thieves such as Hive**

44. It is well known, and the subject of many media reports, that PII/PHI is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data

security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches, Defendant opted to maintain an insufficient and inadequate system to protect the PII/PHI of Plaintiff and Class Members.

45. Plaintiff and Class Members value their PII/PHI, as in today's electronic-centric world, their PII/PHI is required for numerous activities, such as new registrations to websites, or opening a new bank account, as well as signing up for special deals.

46. Legitimate organizations and criminal underground alike recognize the value of PII/PHI. That is why they aggressively seek and pay for it.

47. PII/PHI is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as "dumps." *See All About Fraud: How Crooks Get the CVV*, Krebs on Security (April 26, 2016), <https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/>.

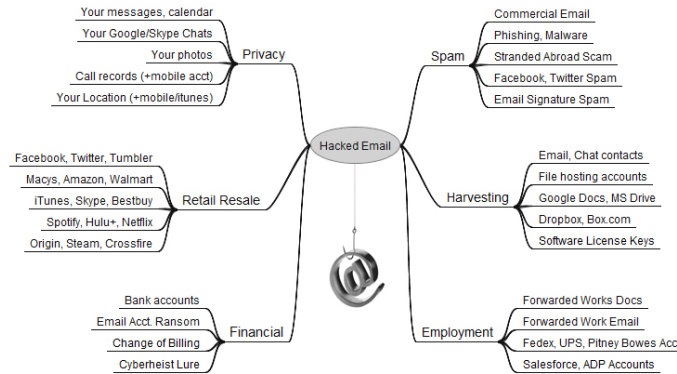
48. Once someone buys PII/PHI, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

49. In addition to PII/PHI, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.<sup>12</sup>

---

<sup>12</sup> *Identity Theft and the Value of Your Personal Data*, Trend Micro (Apr. 30, 2015), <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data>. (last accessed November 8, 2022.)

50. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.<sup>13</sup>



51. Hacked information can also enable thieves to obtain other personal information through “phishing.” According to the Report on Phishing available on the United States, Department of Justice’s website: “AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers.”<sup>14</sup>

## H. The Data Breach Has and Will Result in Additional Identity Theft and Identity

### Fraud

52. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII/PHI of Plaintiff and the Class Members. The ramification of Defendant’s failure to keep Plaintiff and the Class Members’ data secure is severe.

<sup>13</sup> Brian Krebs, *The Value of a Hacked Email Account*, Krebs on Security (June 13, 2013), <https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>. (last accessed November 8, 2022).

<sup>14</sup> *Report on Phishing* (Oct. 2006), [https://www.justice.gov/archive/opa/docs/report\\_on\\_phishing.pdf](https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf) (last accessed November 8, 2022).

53. Between 2005 and 2019, at least 249 million individuals were affected by health care data breaches.<sup>15</sup> In 2019 alone, over 505 data HIPAA data breaches were reported, resulting in over 41 million healthcare records being exposed, stolen, or unlawfully disclosed.<sup>16</sup> The frequency and severity of healthcare data breaches has only increased with time. 2021 was reported as the “worst ever year” for healthcare data breaches—with at least 44,993,618 healthcare records having been exposed or stolen across 585 breaches.<sup>17</sup>

54. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice’s Bureau of Justice Statistics (“BJS”) found that “among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems.”<sup>18</sup> In fact, the BJS reported, “resolving the problems caused by identity theft [could] take more than a year for some victims.” *Id.*

#### **I. Annual Monetary Losses from Identity Theft are in the Billions of Dollars**

55. Javelin Strategy and Research reports that losses from identity theft reached \$21 billion in 2013. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO, Report to Congressional Requesters (June 2007), <http://www.gao.gov/new.items/d07737.pdf>. (last accessed November 8, 2022.)

---

<sup>15</sup> *Healthcare Data Breaches: Insights and Implications*, National Library of Medicine (May 13, 2020), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/>. (last accessed November 8, 2022).

<sup>16</sup> *December 2019 Healthcare Data Breach*, HIPAA Journal (Jan 21, 2020), <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed November 8, 2022).

<sup>17</sup> “Largest Healthcare Data Breaches of 2021,” HIPAA Journal (Dec. 30, 2021), <https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/> (last accessed November 8, 2022).

<sup>18</sup> See *Victims of Identity Theft*, U.S. Department of Justice (September 2015, revised November 13, 2017), <https://bjs.ojp.gov/content/pub/pdf/vit14.pdf> (last accessed November 8, 2022).

56. This is particularly the case with HIPAA data breaches such as Empress's, as the information implicated, such as social security numbers of medical history, cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information for years to come. Indeed, medical identity theft are one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.<sup>19</sup> Victims of medical identity theft "often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."<sup>20</sup>

57. Indeed, a study by Experian found that the average total cost of medical identity theft is "nearly \$13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.<sup>21</sup> Victims of healthcare data breaches often find themselves "being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores."<sup>22</sup>

58. Plaintiff and the Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any financial or identity fraud they suffer.

#### **J. Plaintiff and Class Members Suffered Damages**

59. The exposure of Plaintiff and Class Members' PII/PHI to unauthorized third-party hackers was a direct and proximate result of Empress's failure to properly safeguard and protect Plaintiff and Class Members' PII from unauthorized access, use, and disclosure, as required by and state and federal law. Upon information and belief, the data breach was also a result of Empress's failure to establish and implement appropriate administrative, technical, and physical

---

<sup>19</sup> Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), <https://khn.org/news/rise-of-identity-theft/>. (last accessed November 8, 2022).

<sup>20</sup> *Id.*

<sup>21</sup> *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>. (last accessed November 8, 2022).

<sup>22</sup> *Id.*

safeguards to ensure the security and confidentiality of Plaintiff and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their contracts and federal statute and regulation.

60. Plaintiff and Class Members' PII/PHI is private and sensitive in nature and was inadequately protected by Empress. Empress did not obtain Plaintiff and Class Members' consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

61. As a direct and proximate result of Empress's wrongful actions and inaction and the resulting data breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, paying for credit and identity monitoring services, spending time on credit and identity monitoring, placing "freezes" and "alerts" with credit reporting agencies, contacting their personal, financial and healthcare institutions, closing or modifying personal, financial or healthcare accounts, and closely reviewing and monitoring their credit reports, financial accounts and healthcare accounts for unauthorized activity.

62. Plaintiff has also lost the value of her PII/PHI. PII/PHI is a valuable commodity, as evidenced by numerous companies which purchase PII from consumers, such as UBDI, which allows its users to link applications like Spotify, Twitter, or Apple Health and opt-in to paid opportunities to earn income, and Brave, which uses a similar business model, and by market-based pricing data involving the sale of stolen PII across multiple different illicit websites.

63. Top10VPN, a secure network provider, has compiled pricing information for stolen PII, including \$160.15 for online banking details, \$35.00 for credit reports, and \$62.61 for passports. Standalone Yahoo email accounts have been listed for as little as \$0.41, while banking logins are in the range of \$500, and verified Paypal accounts with high balances are listed at as much as \$2,000.

64. In addition, Privacy Affairs, a cyber security research firm, has listed the following prices for stolen PII:

U.S. driving license, high quality:	\$550
Auto insurance card:	\$70
AAA emergency road service membership card:	\$70
Wells Fargo bank statement:	\$25
Wells Fargo bank statement with transactions:	\$80
Rutgers State University student ID:	\$70

65. Empress's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff and Class Members' PII/PHI, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. The improper disclosure and theft of their PII/PHI;
- b. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII/PHI being exposed to and misused by unauthorized third-party hackers;
- c. The untimely and inadequate notification of the data breach;
- d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and
- e. Ascertainable losses in the form of deprivation of the value of their PII/PHI, for which there is a well-established national and international market.

#### **CLASS ACTION ALLEGATIONS**

66. Plaintiff brings this action on their own behalf and pursuant to the Federal Rules of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4). Plaintiff intends to seek certification of a Class defined initially as follows:

All persons residing in the State of New York who received a data breach notice informing them that their PII/PHI had been breached by unauthorized third parties as a result of Empress's data breach.

67. Excluded from each of the above Class is Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judge and the court personnel in this case and any members of their immediate families. Plaintiff reserves the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded or otherwise modified.

68. *Numerosity*, Fed. R. Civ. P. 23(a)(1): The members of the Class are so numerous that the joinder of all members is impractical. At this present moment, the Class is comprised of at least 318,558 individuals. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control, such as reservation receipts and confirmations.

69. *Commonality*, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;
- b. Whether Defendant violated common and statutory by failing to implement reasonable security procedures and practices;
- c. Which security procedures and which data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;

- d. Whether Defendant knew or should have known of the security breach prior to the disclosure;
- e. Whether Defendant has complied with any implied contractual obligation to use reasonable security measures;
- f. Whether Defendant's acts and omissions described herein give rise to a claim of negligence;
- g. Whether Defendant knew or should have known of the security breach prior to its disclosure;
- h. Whether Defendant had a duty to promptly notify Plaintiff and Class Members that their PII was, or potentially could be, compromised;
- i. What security measures, if any, must be implemented by Defendant to comply with its duties under state and federal law;
- j. The nature of the relief, including equitable relief, to which Plaintiff and the Class Members are entitled; and
- k. Whether Plaintiff and the Class Members are entitled to damages, civil penalties, and/or injunctive relief.

70. *Typicality*. Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI/PII, like that of every other Class Member, was collected by Defendant during its ordinary course of business and then subsequently misused and/or disclosed by Defendant.

71. *Adequacy of Representation*, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff has retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiff intends to prosecute this action vigorously. Plaintiff's claims are typical of the claims of other members of the Classes and Plaintiff has the same non-conflicting interests as the other Class Members. Therefore, the interests of the Classes will be fairly and adequately represented by Plaintiff and his counsel.

72. *Superiority of Class Action*, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

73. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied.

74. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

## **CAUSES OF ACTION**

### **FIRST CAUSE OF ACTION**

#### **Negligence**

75. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 74 inclusive, of this Complaint as if set forth fully herein.

76. Defendant requires any individual that uses its services to provide their PII and PHI to Defendant. Defendant collects and stores this PII and PHI as a part of its regular business activities, and for its own pecuniary gain.

77. Defendant owed Plaintiff and the Class Members a duty of care in the handling of its patient's PII. This duty included, but was not limited to, keeping that PII secure and preventing disclosure of the PII to any unauthorized third parties. This duty of care existed independently of Defendants' contractual duties to Plaintiff and the Class Members. Under the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Defendant is obligated to incorporate adequate measures to safeguard and protect PII that is entrusted to them in their ordinary course

of business and transactions with customers.

78. Pursuant to the Federal Trade Commission Act (15 U. S. C. §45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the businesses' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders from these actions further clarify the measures businesses are required to undertake in order to satisfy their data security obligations.<sup>23</sup>

79. Additional industry guidelines which provide a standard of care can be found in NIST's *Framework for Improving Critical Infrastructure Cybersecurity*.<sup>24</sup> NIST's Framework identifies seven steps for establishing or improving a cybersecurity program (section 3. 2). Those steps are:

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The

---

<sup>23</sup> Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> (last accessed November 8, 2022).

<sup>24</sup> "Framework for Improving Critical Infrastructure Cybersecurity," National Institute for Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf> (last accessed November 8, 2022).

organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce,

necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

80. In addition to their obligations under federal regulations and industry standards, Defendant owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiff and the Class Members.

81. Defendant owed a duty to Plaintiff and the Class Members to design, maintain, and test their internal data systems to ensure that the PII/PHI in Defendant's possession was adequately secured and protected.

82. Defendant owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in its custodianship, including adequately training its employees and others who accessed PII/PHI within its computer systems on how to adequately protect PII/PHI.

83. Defendant owed a duty to Plaintiff and the Class Members to implement processes

or safeguards that would detect a breach of their data security systems in a timely manner.

84. Defendant owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

85. Defendant owed a duty to Plaintiff and the Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material consideration in Plaintiff and Class Members' decisions to entrust their PHI/PII to Defendants.

86. Defendant owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when data breaches occur.

87. Defendant owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems. Defendant collected PII from Plaintiff and the Class Members. Defendants knew that a breach of its data systems would cause Plaintiff and the Class Members to incur damages.

88. Defendants breached its duties of care to safeguard and protect the PII/PHI which Plaintiff and the Class Members entrusted to it. Upon information and belief, Defendant adopted inadequate safeguards to protect the PII/PHI and failed to adopt industry-wide standards set forth above in its supposed protection of the PII/PHI. Defendant failed to design, maintain, and test its computer system to ensure that the PII/PHI was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach.

89. Defendant breached the duties set forth in 15 U.S.C. §45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. §45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Member's PII/PHI. In

violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their network's vulnerabilities; and failed to implement policies to correct security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identify and address security gaps.

90. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

91. As a direct and proximate result of Defendant's failure to adequately protect and safeguard the PII, Plaintiff and the Class members suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiff and the Class members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiff and Class Members of the data breach until weeks had passed. In addition, Plaintiff and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

92. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

## **SECOND CAUSE OF ACTION**

### **Breach of Implied Contract**

93. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 92, inclusive, of this Complaint as if set forth fully herein.

94. Plaintiff and Class Members entered into agreements for medical treatment with Defendant. In making those agreements, Defendant solicited and invited Plaintiff and Class Members to provide their PII and PHI to Defendant as requirement of receiving service. Plaintiff

and Class and Members accepted Defendant's offers and provided their PII and PHI to enter the agreements. Inherent within those agreements was an implied contractual obligation that Defendant would implement reasonable and adequate data security to safeguard and protect the PII and PHI entrusted to them by Plaintiff and Class Members from unauthorized disclosure.

95. Thus, when Plaintiff and Class Members provided their PII and PHI to Defendant in exchange for medical services, they entered into implied contracts with Defendant under which Defendant agreed to and was obligated to reasonably protect their PII and PHI. Plaintiff and Class provided payment to Defendant, as well as their PII and PHI, under the reasonable but mistaken belief that any money they paid to Defendant in connection to its provision of medical services would be used in part to provide reasonable and adequate data security for their PII and PHI.

96. This implied contract is acknowledged and memorialized in Defendant's customer-facing documents, including, *inter alia*, Defendant's "Notice of Privacy Practices," wherein Defendant promises that "we respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times."

97. Defendant did not provide reasonable and adequate data security for Plaintiff and Class Member's PII and PHI, and instead caused it to be disclosed to unauthorized third-party hackers. Defendant did not comply with federal statute and regulation and did not comply with industry data security standards. In doing so, Defendant materially breached their obligations under implied contract.

98. That Defendant would implement such reasonable and adequate data security was a material prerequisite to the agreements between Plaintiff and Class Members. Reasonable consumers value the privacy of their PII and PHI, and do not enter into agreements for medical services with healthcare providers which are known not to protect customer data. Accordingly, Plaintiff and Class Members would not have entered into agreements with Defendant and would not have provided them with their sensitive PII and PHI, had they known that Defendant would not implement such reasonable and adequate data security.

99. As a result of Defendant's breach, Plaintiff and Class Members have lost the benefit of their bargains. Plaintiff and Class members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII/PHI, and would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII/PHI. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

100. Plaintiff and Class Members fully performed their obligations under the implied contract by providing their PII/PHI and making payments to Defendant.

101. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

### **THIRD CAUSE OF ACTION**

#### **Violation of New York Gen. Bus. Law §349 – Deceptive Acts and Practices**

102. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 101 inclusive of this Complaint as if set forth fully herein.

103. Defendant has engaged in deceptive acts or practices in the conduct of its business. Specifically, Defendant engaged in deceptive acts or practices by, *inter alia*: misrepresenting to Plaintiff and Class Members that it would protect Plaintiff and Class Member's PII and PHI from unauthorized disclosure, failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Member's PII and PHI, failing to identify and remediate foreseeable data security vulnerabilities in its own systems, failing to disclose and concealing the material fact that its data security systems could not and would not reasonably and adequately protect Plaintiff and Class Member's PII and PHI, and failing to disclose and concealing the material fact that its data security systems were not compliant with federal statute, regulation and industry cybersecurity standards.

104. Defendant's misconduct is consumer oriented. Specifically, Defendant makes representations to consumers that it will protect any sensitive PII and PHI that they provide to Defendant. Defendant makes these representations in, but not limited to, its "Notice of Privacy Practices," wherein it promises that "[w]e respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times." This promise was misrepresentative and misleading, as Defendant did not implement strict policies of confidentiality that their staff followed at all times, as evidenced by its breach of almost 390,000 individual's sensitive PII/PHI.

105. Defendant's misconduct is likely to deceive reasonable consumers, including Plaintiff and Class Members. Reasonable consumers reasonably expect that healthcare providers that they enter into agreements for medical services will take reasonable and adequate steps to protect any sensitive PII/PHI that they provide to those providers during the ordinary course of business. Reasonable consumers do not expect that healthcare providers will allow their sensitive PII/PHI to be obtained by unauthorized and malicious third-party hackers.

106. Defendant's misconduct is material to reasonable consumers, including Plaintiff and Class Members. Reasonable consumers do not expect that healthcare providers will disclose their sensitive PII/PHI to unauthorized and malicious third-party hackers, and do not enter into agreements or provide their PII/PHI to providers that do so. Plaintiff and Class Members were thus materially misled by Defendant.

107. Defendant's deceptive and unlawful practices affect the public interest and consumers at large. Consumers who desire to obtain healthcare services from Defendant, but who are unaware of Defendant's inability or refusal to implement adequate and reasonable security measures for customer PII/PHI, are highly likely to be and are materially misled.

108. As a direct and proximate cause of Defendant's violation of the New York General Business Law, Plaintiff and Class Members have suffered injury that they could not have reasonably avoided, and are entitled to damages in an amount to be proven at trial, including actual damages (or \$50 per class member, whichever is higher), treble damages, and punitive damages,

as well as attorney's fees and costs.

109. Plaintiff also brings this action to enjoin the unlawful acts and practices set forth herein.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually and on behalf of all of the Class Members, respectfully requests that the Court enter judgment in his favor and against Defendant as follows:

1. For an Order certifying the Classes as defined herein and appointing Plaintiff and his Counsel to represent the Classes;
2. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII/PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
3. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of PII compromised.
4. For an award of actual damages, statutory damages and compensatory damages, in an amount to be determined at trial;
5. For an award of punitive and treble damages, in an amount to be determined at trial;
6. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and
7. For such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: November 29, 2022

Respectfully submitted,

By: s/ Thiago M. Coelho  
Thiago M. Coelho  
*pro hac vice pending*  
**WILSHIRE LAW FIRM, PLC**  
3055 Wilshire Blvd., 12th Floor  
Los Angeles, CA 90010  
T: (213) 381-9988  
F: (213) 381-9989  
E: thiago@wilshirelawfirm.com

Daniel A. Schlanger  
**SCHLANGER LAW GROUP LLP**  
80 Broad Street, Suite 1301  
New York, NY 10004  
T: 212-500-6114  
F: 646-612-7996  
E: dschlanger@consumerprotection.net

*Attorneys for Plaintiff and the Putative Classes*